NAVAL
POSTGRADUATE
SCHOOL

MONTEREY, CALIFORNIA

THESIS

ORGANIZATIONAL CHANGE FOR THE INTELLIGENCE COMMUNITY SUPPORTING MARITIME HOMELAND SECURITY AND DEFENSE: DEVELOPING A DOMESTIC MARITIME INTELLIGENCE NETWORK

by

Bradley J. Storey

September 2003

Thesis Advisor: D. C. Boger
Second Reader: R. M. Brown

Approved for public release; distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2003	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Organizational Change for the Intelligence Community Supporting Maritime Homeland Security and Defense: Developing a Domestic Maritime Intelligence Network			**5. FUNDING NUMBERS**
6. AUTHOR(S) Bradley J. Storey			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT **Approved for public release; distribution is unlimited.**			**12b. DISTRIBUTION CODE**

13. ABSTRACT ***(maximum 200 words)***

Since the beginning of the twentieth century, the United States has conducted the missions of Homeland Security and Defense abroad, rather than within its borders. While keeping conflict outside of our borders is preferred, the terrorist attacks that occurred on September 11, 2001 have illustrated that this is not always possible. The missions of Maritime Homeland Security and Defense have gained significant importance in the overall national security of the United States. In order to effectively support these missions, an effective intelligence apparatus must exist which is adapted to the Information Age. Terrorist groups are using the network forms of organization, with significant advantages over traditional hierarchies within the U.S. government. Effectively organizing the various agencies involved in domestic maritime intelligence will require rapid movement of intelligence to the operational customer. The most effective way to organize these agencies to support Maritime Homeland Security and Defense is to create a domestic maritime intelligence network.

14. SUBJECT TERMS Maritime Homeland Security, Maritime Homeland Defense, Intelligence, Network, Organizational Structure, Terrorism			**15. NUMBER OF PAGES** 55
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited.

ORGANIZATIONAL CHANGE FOR THE INTELLIGENCE COMMUNITY SUPPORTING MARITIME HOMELAND SECURITY AND DEFENSE: DEVELOPING A DOMESTIC MARITIME INTELLIGENCE NETWORK

Bradley J. Storey
Lieutenant, United States Navy
B.S., United States Naval Academy, 1998

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS TECHNOLOGY

from the

NAVAL POSTGRADUATE SCHOOL
September 2003

Author: Bradley J. Storey

Approved by: D. C. Boger
Thesis Advisor

R. M. Brown
Second Reader

D. C. Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Since the beginning of the twentieth century, the United States has conducted the missions of Homeland Security and Defense abroad, rather than within its borders. While keeping conflict outside of our borders is preferred, the terrorist attacks that occurred on September 11, 2001 have illustrated that this is not always possible. The missions of Maritime Homeland Security and Defense have gained significant importance in the overall national security of the United States. In order to effectively support these missions, an effective intelligence apparatus must exist which is adapted to the Information Age. Terrorist groups are using the network forms of organization, with significant advantages over traditional hierarchies within the U.S. government. Effectively organizing the various agencies involved in domestic maritime intelligence will require rapid movement of intelligence to the operational customer. The most effective way to organize these agencies to support Maritime Homeland Security and Defense is to create a domestic maritime intelligence network.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

Throughout recent history, the United States has focused its Homeland Security and Defense missions away from the domestic theater. A new threat dimension has arisen from the Information Age, which now challenges the United States in its own backyard. The terrorist attacks of September 11, 2001 illustrate the seriousness of this new threat environment. Within this new atmosphere of significant domestic terrorist threat, the missions of MHLS and MHLD have risen in importance as never before. Intelligence support to each mission forces a significant change in the way that the intelligence community conducts business. A new way of organizing the intelligence community can yield significant advances in support to MHLS and MHLD. This reorganization must develop a highly networked domestic maritime intelligence community.

While the missions of HLS and HLD reflect certain differences in definition, the overall goal of each is to protect the homeland of the United States against terrorist attacks. The recent creations of DHS and USNORTHCOM have provided a C2 structure with which to conduct these two missions. Under each respective command, USCG has the lead for MHLS and NAVNORTH takes over when conducting MHLD. The resulting C2 organizations for both MHLS and MHLD are hierarchal in nature.

The theory of Netwar, as described by John Arquilla and David Ronfeldt, describes the evolution of network organizations based on advances made in the information revolution. This theory proposes a progression towards the complex all-channel network form. Hierarchies have significant difficulty fighting networks. Therefore, with the enemy defined as a hybrid all-channel terrorist network targeting the homeland of the U.S., it will become increasingly difficult for a hierarchal intelligence community to effectively monitor and predict this enemy's likely courses of action.

With all of these ideas put together, it is clear that organizational change must occur in intelligence support to MHLS and MHLD. This thesis argues that the most effective way to organize these intelligence communities is to merge them both into a domestic maritime intelligence network.

To monitor and predict enemy actions in MHLS and MHLD, a hybrid form of the all-channel network should be developed for use by the domestic maritime intelligence community. This network should be all-channel in form, with certain hub network nodes. In addition, the ability to tailor, filter, and fuse information at the strategic, operational, and tactical levels must be implemented. In order to effectively accomplish this task, domestic maritime intelligence must attain a joint-interagency form. The foundation beneath this intelligence network encompasses the formal implementation of three main ideas:

- Willingness to actively share information at all levels.
- Creation of formal liaison and interagency communication.
- Elimination of the competitive paradigm between intelligence agencies.

The implementation of these ideas will allow a hybrid all-channel network to form in support of MHLS and MHLD.

Within the network, each warfare level must be supported with dedicated intelligence fusion. NMIC should be a dedicated node within the network, responsible for fusing intelligence at the strategic level. MIFC-LANT and MIFC-PAC should be the two nodes in the network primarily focusing on fusion at the operational level. Finally, at the tactical port level, each port should have a JHOC which is responsible for monitoring activity within each port. As with the concept of the all-channel network, all of these nodes must become interconnected, so exchange of information can occur between all levels of intelligence support.

The current intelligence organization has three major issues which impact its ability to adequately support MHLS and MHLD:

- Organizational structure
- Information systems
- Misconceptions of the missions

Within each of these areas there are significant shortfalls which endanger the homeland maritime domain awareness each day. By developing a maritime intelligence network,

creating effective sensors and communications, and truly understanding the missions of MHLS and MHLD, the country can begin to efficiently develop a safer domestic maritime domain.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. OVERVIEW

Since the beginning of the twentieth century, the United States has conducted the missions of Homeland Security and Defense abroad, rather than within its borders. The defense of American citizens and interests has often led to conflict on foreign soil. While keeping conflict outside of our borders is preferred, the terrorist attacks that occurred on September 11, 2001 have illustrated that this is not always possible. American citizens expect and demand an effective domestic security and defense system in this new threat environment. Therefore, the intelligence community must redefine its role in defense of the homeland, and take steps to reorganize to sufficiently support the missions of Homeland Security and Defense.

Within the realm of Homeland Security and Defense lies the domestic maritime theater. The missions of Maritime Homeland Security (MHLS) and Maritime Homeland Defense (MHLD) are vital to the national security of the United States. Given the large number of organizations involved, intelligence support to these missions requires a great deal of reorganization and improved interoperability. While it is important to acknowledge the current organizational doctrine for the intelligence community, the intent of this thesis is to provide insight into needed improvements to intelligence organizations which will help define the renewed national focus on MHLS and MHLD. The overall objective is to provide answers to the following questions:

- How should intelligence support to MHLS and MHLD be organized in order to best support the strategic, operational, and tactical environments? What are the roles and responsibilities of Coast Guard Intelligence and Naval Intelligence in MHLS and MHLD?
- What gaps and obstacles exist in the current intelligence organizational structure that might impede the missions of MHLS and MHLD?

The overall idea involved in answering these questions is that intelligence support to both MHLS and MHLD is essentially the same. Effectively organizing the various agencies involved in supporting these missions will require rapid movement of

intelligence to the operational customer. The most effective way to organize these agencies to support MHLS and MHLD is to create a maritime intelligence network.

B. STRUCTURE OF THESIS

Chapter II reviews the roles and responsibilities of various organizations within MHLS and MHLD, as defined by the President of the United States. Homeland Security and Homeland Defense are defined and related to the maritime environment. Importantly, the Command and Control (C2) structure is presented in order to identify combatant commanders and lead organizations for each mission. While the intelligence organizational structure should not be dependent on which commander is being supported, it is important to outline the focus and flow of the intelligence support to each mission.

Chapter III examines the theories of network organizations. It discusses the various types of networks and how they operate. The chapter compares hierarchal organizations to networks and points out the advantages of networks over hierarchies. In addition, the chapter will reveal how the perceived enemy is most likely organized, and how the intelligence organizational structure supporting MHLS and MHLD must be a network in order to be successful.

Chapter IV presents an organizational blueprint to effectively make MHLS and MHLD intelligence into a successful network. It defines roles and responsibilities of all intelligence organizations within the network to support the strategic, operational, and tactical environments. This chapter defines the roles of Coast Guard and Naval Intelligence to develop a Common Intelligence Picture (CIP) for the domestic maritime theater. It also provides insights into the current gaps and obstacles in the current organizational structure, and provides recommendations to remedy these shortfalls.

Chapter V provides a conclusion to the discussions made in the previous chapters. It summarizes the analysis of the MLHS and MHLD intelligence process and provides some key points which appear vital to creating an effective intelligence organization that supports each mission.

II. MARITIME HOMELAND SECURITY AND DEFENSE COMMAND AND CONTROL; DEFINING THE CUSTOMER

A. DEFINITIONS

Homeland Security is defined as "a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur"[1] in the *National Strategy For Homeland Security*, released in July 2002. Essentially, this definition outlines a mission requirement to prepare for and proactively prevent terrorist attacks in the U.S. on a day-to-day basis. Therefore, MHLS represents any element of the HLS mission which occurs in the domestic maritime theater.

According to *General Military Training Homeland Defense*, Homeland Defense is defined as "the protection of U.S. territory, sovereignty, domestic population and critical infrastructure through deterrence of and defense against direct attacks as well as management of the consequences of such attacks"[2]. This definition creates a mission to respond to imminent attacks on the homeland, and if necessary, respond to attacks which have already occurred. This makes MHLD the execution of the HLD mission in the domestic maritime theater.

An important point to understand about HLS and HLD is that both missions support the same goal in the end, protection of the homeland of the United States. The main difference lies in the execution of each mission.

B. COMMAND AND CONTROL (C2)

According to the Homeland Security Act of 2002, the Department of Homeland Security (DHS) has the lead role in conducting Homeland Security. As a result of the establishment of DHS, the U.S. Coast Guard (USCG) transitions from the Department of

---

[1] Office of Homeland Security, *National Strategy for Homeland Security*. p. 2. Government Printing Office. July 2002.

[2] Chief of Naval Education and Training, *General Military Training Homeland Defense*. p. 1-5-4. Government Printing Office. 2003.

Transportation to DHS. From a maritime prospective, the Coast Guard represents the lead element within DHS to conduct the mission of MHLS.

Similarly, the Department of Defense (DOD) is directed to assume the lead role in conducting Homeland Defense. As a result of this act, the newly-established unified command U.S. Northern Command (USNORTHCOM) is given the responsibility to conduct the mission of Homeland Defense. This thesis will identify USNORTHCOM as the representative of DOD in Homeland Defense discussions. Under HLD conditions, the U.S. Navy (USN) normally acts as the lead organization for conducting MHLD under USNORTHCOM.

From a joint military operations perspective, the situation is best described in terms of the "Supported Commander" and the "Supporting Commander". When the country is conducting the HLS mission, DHS is the "Supported Commander" and USNORTHCOM is the "Supporting Commander". Conversely, when the country is conducting the HLD mission, USNORTHCOM becomes the "Supported Commander" and DHS becomes the "Supporting Commander". From a doctrinal perspective, the resulting structure gives the Coast Guard the lead in conducting MHLS, and the Navy the lead in conducting MHLD.

This reorganization creates a great deal of ambiguity as to when HLS should transition to HLD, and when it should transition back again. Since there are different agencies taking the lead for each mission, it is often unclear who should be in charge under some circumstance. Differentiating between the two missions projects which agency should take charge, however the decisive point between them is often difficult to interpret, as has been demonstrated in war games.[3] This is obviously an operational concern, however, it should not impact the intelligence process. Since the missions of HLS and HLD support the same end goal, the intelligence support to each mission is identical. The only difference lies in which commander, or "customer", is the focus of the intelligence flow. One of the key concepts to understand in the world of MHLS and MHLD is that the intelligence process supporting each mission is the same.

[3] Maritime Homeland Security and Defense War Game. Naval Postgraduate School. 2003.

C. CURRENT MHLD C2 ORGANIZATIONAL STRUCTURE

As was stated before, USNORTHCOM has the responsibility of conducting MHLD according to the implemented modifications to the Unified Command Plan on October 1, 2002. This established USNORTHCOM Headquarters at Peterson AFB in Colorado Springs, CO. As with any unified command, the command structure of USNORTHCOM is divided into component commanders which reflect the basic missions within USNORTHCOM. These component commanders are the Joint Forces Maritime Component Commander (JFMCC), Joint Forces Air Component Commander (JFACC), and the Joint Forces Land Component Commander (JFLCC). Each of these organizations have their subcomponents, however, the C2 structure for the JFMCC is the only one that will be presented here, since the concentration is on the mission of MHLD.

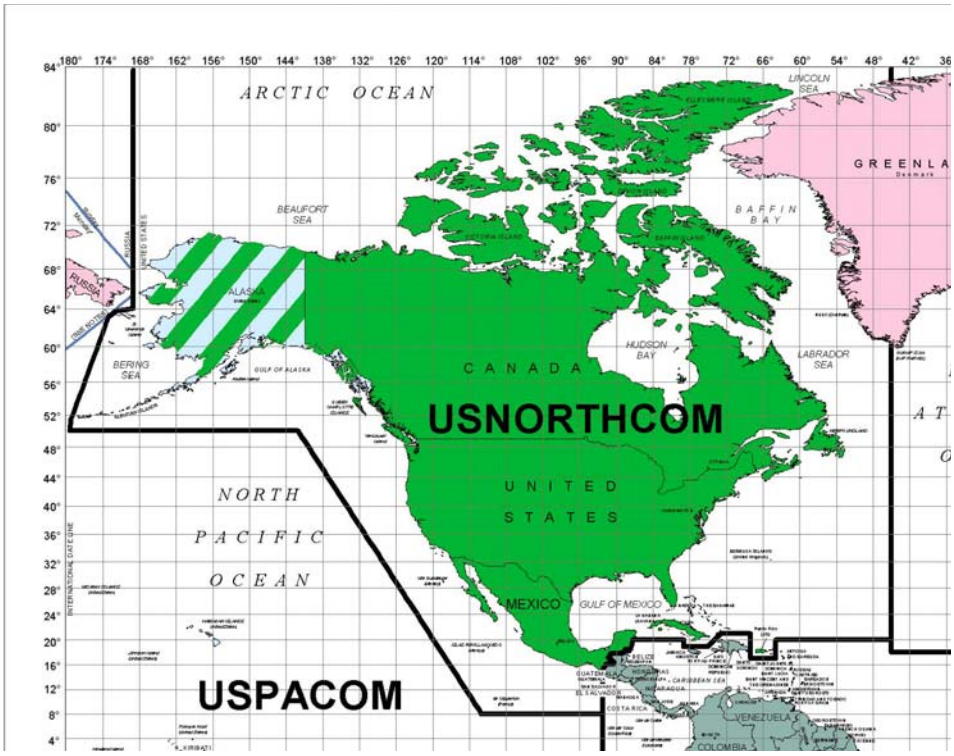
One important and unique difference between USNORTHCOM and the other unified commands is that it has no forces regularly assigned to it. Therefore, USNORTHCOM represents a "skeleton" infrastructure which has no ability to conduct operations without the explicit authorization of the Secretary of Defense (SECDEF).[4] Without any forces actually assigned to USNORTHCOM, it is sometimes difficult to understand the component commands due to the fact that the staff organizations involved often have several names and responsibilities to other commanders until SECDEF authorization is given to assign forces to USNORTHCOM.

The JFMCC for USNORTHCOM is one of these organizations with several names, missions, and commanders. The actual name given to the USNORTHCOM JFMCC is US Naval Forces Northern Command (NAVNORTH), located in Norfolk, VA. This command is also known as Commander Fleet Forces Command (CFFC) and Commander US Atlantic Fleet (CLF), and is regularly assigned for control under Joint Forces Command (JFCOM) until forces are assigned to USNORTHCOM. Further discussion will refer to the JFMCC as NAVNORTH in order to avoid further confusion, since the topic at hand is MHLD. It is important to note that Coast Guard forces can be assigned to a JFMCC according to the Unified Command Plan. CFFC and CLF are solely Navy organizations. In addition, with USN taking the lead in MHLD under

[4] USNORTHCOM. "Who We Are-Our Team". www.northcom.mil. July 2003.

USNORTHCOM, NAVNORTH will be the organization within USN which will conduct MHLD. Figure 1 illustrates the domain for which USNORTHCOM and its subcomponents have responsibility.

Figure 1. USNORTHCOM Area of Responsibility.

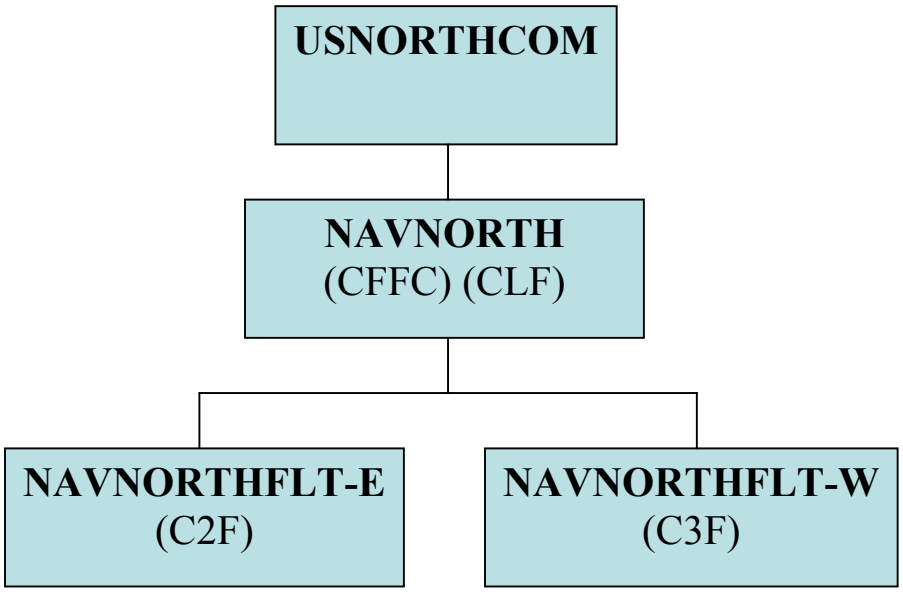


Source: www.defenselink.mil

Subcomponents of NAVNORTH have been broken down into NAVNORTH Fleet East (NAVNORTHFLT-E), located in Norfolk, VA, and NAVNORTH Fleet West (NAVNORTHFLT-W), located in San Diego, CA. This organizational method assigns responsibility to each continental US coast to a different subcommander. These organizations also have other names and responsibilities until forces are assigned to USNORTHCOM. NAVNORTHFLT-E is also known as Commander Second Fleet (C2F), which is regularly assigned control under Commander US Atlantic Fleet (CLF). NAVNORTHFLT-W has a similar arrangement, being also called Commander Third Fleet (C3F). However, C3F regularly operates under Commander US Pacific Fleet (CPF) and US Pacific Command (USPACOM).[5] Figure 2 illustrates how these component commands are organized under USNORTHCOM during MHLD missions.

[5] USNORTHCOM MDA Conference. USNORTHCOM. 2003.

Figure 2. Current USNORTHCOM Maritime C2 Structure.



Source: USNORTHCOM MDA Conference

The resulting organizational structure within USNORTHCOM is very hierarchal in nature, and often quite confusing due to the fact that no forces are assigned on a regular basis. In addition, component and subcomponent commanders under USNORTHCOM have competing responsibilities to other Unified Commands until actually assigned the mission of MHLD. Many problems result from this structure, including training, funding, and C2 in general. The problems in the operational C2 organizational structure are not the overall focus of this research, since the thesis discussion analyzes the intelligence organizational structure supporting MHLD. However, it is important to note that the operational C2 organization is the "customer" of the intelligence, and thus any shortfalls within that organization will affect the intelligence process.

D. CURRENT MHLS C2 ORGANIZATIONAL STRUCTURE

The creation of DHS, and the assignment of USCG to DHS, gave USCG the lead in the MHLS mission. Due to the Coast Guard's historical role in conducting MHLS, a

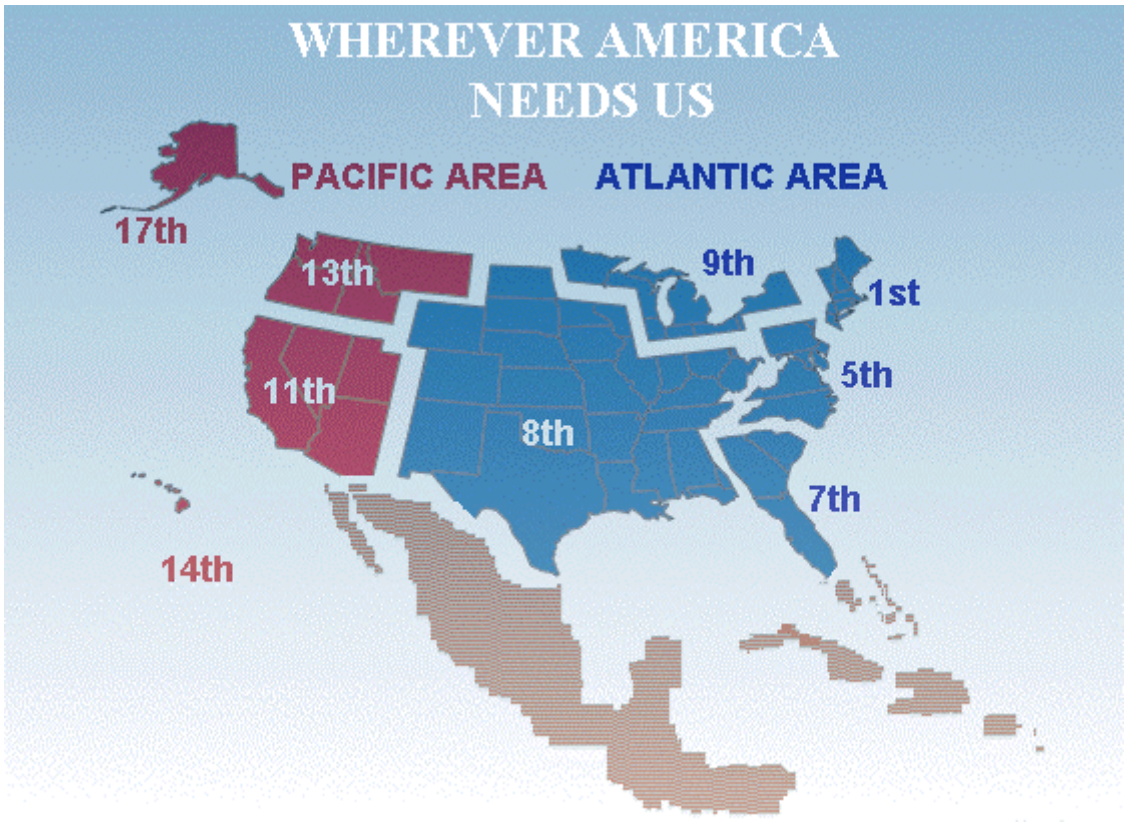
massive C2 reorganization was not required within the organization. However, the Coast Guard focused much of its efforts on missions such as lifesaving, environmental security, and navigation. After the terrorist attacks of September 11th, MHLS became the highest priority. In addition, forces are regularly assigned under USCG, and therefore component and subcomponent commands do not have multiple names and commanders. This makes the C2 process under USCG more clear and practiced. The Commandant of the Coast Guard represents DHS in the MHLS mission.

Much like the NAVNORTHFLT-E/W organizations, USCG is broken down into component commands for each coast. Commander USCG Atlantic Area (LANTAREA), located in Portsmouth, VA, directs USCG operations on the east coast of the US and in the the Gulf of Mexico. Commander USCG Pacific Area (PACAREA), located in Alameda, CA, directs USCG operations on the west coast of the US, to include Alaska, Hawaii, and the Eastern Pacific region. These commanders are regularly assigned forces, and report directly to the Commandant of the Coast Guard.

Subcomponents exist within both LANTAREA and PACAREA, known as USCG Districts. LANTAREA commands Districts 1, 5, 7, 8, and 9 (D-1, D-5, D-7, D-8, and D-9). PACAREA commands Districts 11, 13, 14, and 17 (D-11, D-13, D-14, and D-17).[6] These districts also carry out responsibility and authority over inland bodies of water and waterways. Figure 3 illustrates the Area of Responsibility for USCG and its subcomponents. Figure 4 shows the organizational C2 structure for the DHS while conducting MHLS.

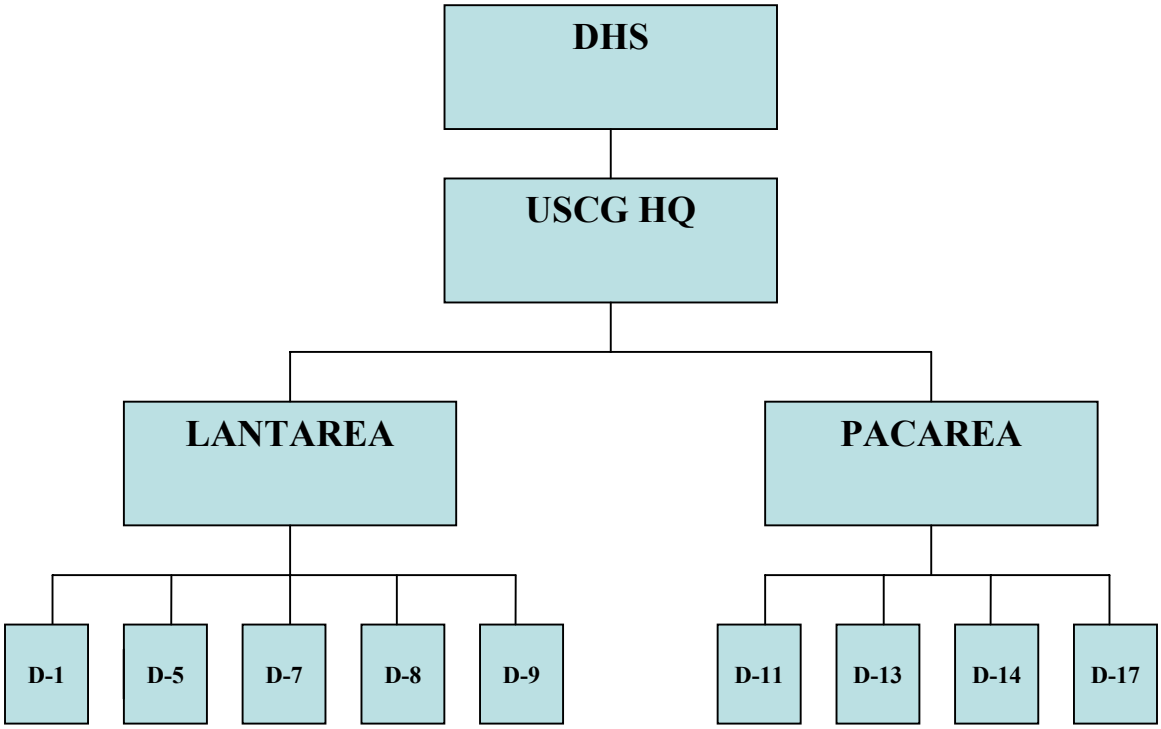
6 USNORTHCOM MDA Conference.

Figure 3. USCG Areas of Responsibility.



Source: www.uscg.mil

Figure 4. Current USCG C2 Structure.



Source: USNORTHCOM MDA Conference

Once again, the organizational structure under USCG is a hierarchy. Although the chain of command is not as confusing as USNORTHCOM, and training and funding are not affected by it, the C2 process for this type of organization will still have problems confronting network organizations. It is worth repeating that while the operational C2 structure is not being analyzed in this study, it does however, have direct implications on intelligence support to this "customer" as well.

E. SUMMARY

The definitions of HLS and HLD illustrate that the overall goal resulting from each mission is the same, protection of the homeland of the United States. While execution of each mission is conducted under different authority, it is important to understand which organization is in charge in order to decide where intelligence support must be provided in a given situation. It is quite clear that both the new DHS and new

USNORTHCOM are organized into hierarchal forms. This is an operational issue which can have negative repercussions given the network organization of the enemy. However, these examples are only provided to illustrate the "customer" of intelligence support to MHLS and MHLD. The true intent of this study is to show that by creating an MHLS and MHLD intelligence network, it will prove to bring impressive clarity to the operational picture for NAVNORTH and USCG.

III. UNDERSTANDING THE WORLD OF NETWAR AND NETWORK ORGANIZATIONS

A. THE THEORY OF NETWAR

The discussions in this chapter revolve around an emerging method of organizational theory known as "Netwar". John Arquilla and David Ronfeldt define Netwar as "an emerging mode of conflict (and crime) at societal levels, short of traditional military warfare, in which the protagonists use network forms of organization and related doctrines, strategies, and technologies attuned to the information age"[7]. This idea is fed by the ongoing advances in information technology, but is more about organizational practice than technology itself. The revolution in information technology favors and strengthens the network organizational principle, and leaves traditional hierarchal organizations at a disadvantage.[8] Therefore, as the technology advances and is used, organizational structure should reflect more efficient ways of using these technologies in order to gain the advantage.

Grasping the concept of Netwar forces one to look at the world from a different perspective. In warfare, the hierarchal pyramid dominates the development of historical military structure. In fact, great historical success in global conflict has been attained by using this form of organization. It is easy to take the view that changing a historically successful organizational practice may lead to a self-created disadvantage. However, after viewing the drastically changed global environment resulting from growth patterns in the Information Age, it is clear that the future favors a revolution in organizational doctrine.

B. TYPES OF NETWORKS

Networks are comprised of a series of "nodes" which have some ability to pass information. Nodes represent people, places, or organizations that have contact with

---

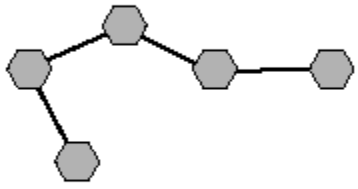
[7] Arquilla, J. and Ronfeldt, D., *Networks and Netwars*, p. 6. RAND, 2001.

[8] Arquilla, 1.

other nodes for information flow. These nodes can be connected through three major types of networks; the chain network, the hub network, and the all-channel network.[9]

The chain or line network is a series of nodes in a line where information passes from one node to the next. Figure 5 shows a visual diagram of the chain network structure. No information passes directly from one end to the other without passing through intermediate nodes.[10] This type of network is fairly simple to create in terms of communication technology. It also can possess a sense of confidentiality between different ends and nodes since direct communication only occurs with the two adjacent nodes. As a result of this series of communication relays, information flow can be slowed and become inaccurate as it passes through each node from end to end. In addition, information flow can be disrupted easily by breaking a link or node in the chain network. Overall, the chain network is the simplest to set up, however, the slowest and most vulnerable to disruption.

Figure 5. Chain Network Structure.



Chain network

Source: ***Networks and Netwars***

The hub, star, or wheel network form uses a central node, or hub, which is connected to several other nodes. Figure 6 illustrates the structure of the hub network.

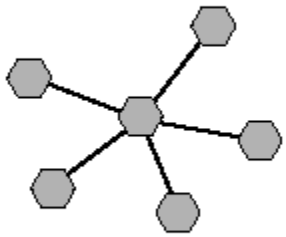
[9] Arquilla, 7-8.

[10] Arquilla, 7.

The resulting organization forces all communications to go through the central node. It is important to clarify that the central node is not a hierarchy, but a common center for information flow between the other nodes in the network.[11] The hub network is a bit more complex in terms of coordinating information passing from origin to destination through the hub. It also allows for faster coordination of information flowing to and from multiple sources without the long trail of nodes present in the chain network. Simultaneous communication to several nodes from the hub is possible, which creates faster flow and more accurate common knowledge between all nodes. The hub requires more diverse communication technology in order to keep up with where information is coming from, and where it needs to go. In addition, centralizing the communication hub to a single point of vulnerability makes the network depend on the preservation of the hub. This presents a clear target to disable the network if the hub can be identified. Overall, the hub network allows for a faster flow rate and common picture, however, it requires more complex technology and is vulnerable to attack of the hub.

[11] Arquilla, 7.

Figure 6. Hub Network Structure.

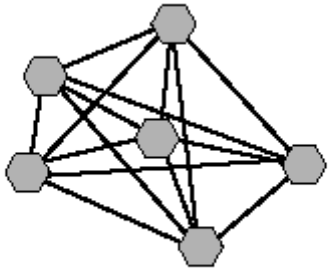


Source: ***Networks and Netwars***

The third type of network is the all-channel or full-matrix network. With this form of network, every node in the network is directly connected to every other node.[12] Figure 7 provides a simple diagram of an all-channel network, however, it is difficult to draw this type of network due to its three-dimensional structure. This type of network is the most complex of all three forms. Directly connecting all nodes together allows for extremely fast information flow from source to destination. In addition, the entire network is not significantly affected if one node is targeted. Information continues to flow around a node if it is eliminated. Overall, the all-channel network is the most efficient means of rapidly passing information to all nodes in the network. This organization requires very advanced technology in order to connect all nodes together, but decentralizes the network to decrease vulnerabilities to targeting.

[12] Arquilla, 8.

Figure 7. All-channel Network Structure.



All-channel network

Source: ***Networks and Netwars***

It is clear that each of these types of networks has its own positive and negative characteristics. Each is also found within the Netwar concept, applying its strengths to various organizations. In addition, hybrid networks exist, which apply two or more of these three basic networks into the overall organization.[13] The hybrid idea allows an organization to tailor its network around various components within the overall network. Networks couple themselves with hierarchies as well. This type of hybrid may weave several hierarchal organizations into a network.[14] The use of hybrids can additionally strengthen a diverse organization by allowing it to adapt its network to support the various operations within the overall organization. Also, applying multiple organizational concepts can provide better organizational preservation by clouding the targeting process.

C. THE PERCEIVED ENEMY ORGANIZATION

Netwar-related adversaries use all three types of networks based on their purposes and goals. Smuggling operations often use the chain network by passing information and products from node to node along the chain. The hub network is often applied at the core

[13] Arquilla, 8.

[14] Arquilla, 8.

of terrorist and criminal organizations. Militant groups often prefer the all-channel network to become decentralized and highly interoperable.[15]

According the definitions of HLS and HLD presented earlier, the enemy is defined as terrorist organizations that target the homeland of the United States. Therefore, the enemy in the missions of MHLS and MHLD is designated as terrorist organizations that threaten the domestic maritime environment of the United States. The key to understanding how the enemy fights is to understand how it is organized.

As was stated earlier, terrorist organizations often use the hub network design. However, as the pace of the information revolution is bringing inexpensive, advanced information technology to the hands of the private sector, hybrid terrorist organizations are developing. These terrorist groups are beginning to couple the all-channel design with the hub network. The major obstacle impeding the formation of an all-channel network is the robust communication and information system that is required.[16] However, the increasingly vast availability of inexpensive information technology is making this movement much easier.

Offensively, the hybrid organization favors flexibility and adaptability.[17] The evolution of swarming tactics among terrorist organizations allows them to remain dispersed until the defining moment of attack. This type of network makes dispersal even easier, and also allows the information flow which is vital to quickly culminate an attack on an enemy's weak point. Swarming allows the network to decide where and when confrontations will occur, thus giving the terrorists the advantage of creating conflict when the situation is favorable to them.

From a defensive standpoint, the hybrid movement renders counter-leadership targeting ineffective.[18] Examples of this are the continued activity of groups such as al-Qaeda and Fedayeen after the apprehension of leading members of both organizations. By eliminating a hub node in the hub network, the overall organization can be damaged.

---

[15] Arquilla, 8.

[16] Arquilla, 10.

[17] Arquilla, 12.

[18] Arquilla, 13.

However, by transitioning to the all-channel design, the network gains diversity and redundancies which can make it more resistant to attack.[19]

The resulting situation creates a blending and blurring of offensive and defensive operations.[20] "Hit and run" tactics are used which frustrate and confuse the opponent. Time and again, these methods give the solid advantage to the hybrid network. To confuse the issue even more, the enemy's network is non-state. This makes it even harder to prosecute due to its presence over many borders. An enemy that is networked in this manner holds a significant organizational advantage over the hierarchal agencies involved in MHLS and MHLD.

D. THE NETWORK VS. THE HIERARCHY

There are major differences between networks and hierarchies as organizational systems, and as with any system, there are advantages and disadvantages of each. However, as a whole, the network holds a much greater organizational advantage over the hierarchy. Arquilla and Ronfeldt make three main points regarding networks and hierarchies:

- "Hierarchies have a difficult time fighting networks."
- "It takes networks to fight networks."
- "Whoever masters the network form first and best will gain major advantages."[21]

These points ring true in various historical examples, and the technology trend is definitely favoring a transition in organizational behavior based on information flow capabilities.

The hierarchy resembles a pyramid form in essence. The pyramid can be broken down into a simplified top, middle, and bottom levels.[22] At the top level is the leader, or small group of leaders, which forms the head of the organization. Below the top level there are a significantly larger number of middle managers, with "sub-managers" that report to them. Finally, the bottom level represents the workforce of the hierarchy that

---

[19] Arquilla, 13.

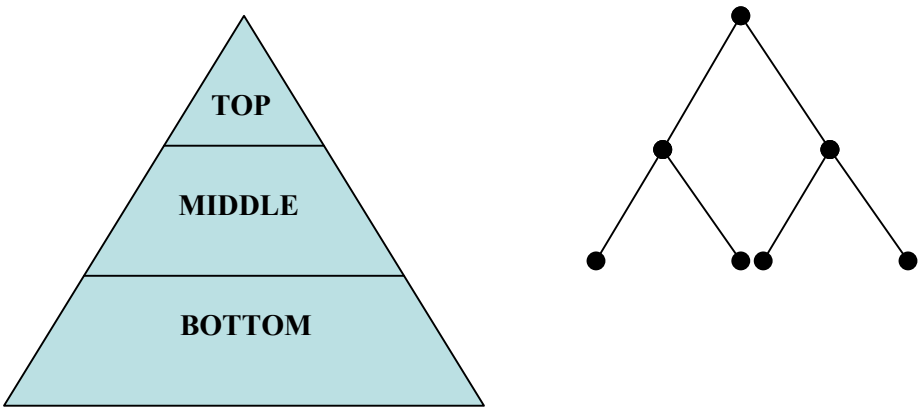
[20] Arquilla, 13.

[21] Arquilla, 15.

[22] Wagner III, J.A. and Hollenbeck, J.R., *Organizational Behavior, Securing Competitive Advantage*, 3d ed., p. 287. Prentice Hall, 1998.

reports to the sub-managers. Overall, the organization is centralized with respect to leadership.[23] While delegation of authority usually occurs between levels, elimination of a leadership element can often drastically affect a hierarchy.

Figure 8. Hierarchal Structure.



In contrast, the network is a very flat organization that does not resemble a pyramid. The design of this type of organization is flat, without a central leadership element.[24] In this case, leadership makes its presence known, but only in limited roles. There may be several leaders within a network, and the idea is to decentralize control and rely on initiative within the network. Therefore the network often appears to have no heads, or multiple heads, depending on how it is set up.[25] The overall body is governed by common goals. To use the perceived enemy as an example, the overall goals are destruction and disruption of the domestic maritime environment. Therefore, any actions aimed at those goals are in line with the organization.

Historically, hierarchies have had a very hard time confronting network organizations. Examples are drug smuggling in Columbia and the Zapatista movement in Mexico.[26] While both forms of organizations may be governed by common goals, the network gains the advantage with speed and efficiency. The hierarchy's centralization of

[23] Wagner, 287.

[24] Arquilla, 9.

[25] Arquilla, 9.

[26] Arquilla, 15.

control forces low-level feedback to climb the "chain of command" in order to eventually have a decision made at the appropriate level. Then, the decision must make its way back down to the low level. In addition, communication and coordination between different low-level groups must occur at the middle level. This greatly slows the speed of information flow. In addition, counter-leadership targeting can have significant impacts on the hierarchy by cutting off the heads of groups and leaving them with little or no communication and coordination.

When supported by an effective information system, a network is much faster and more efficient than a hierarchy. Since there are no top or middle levels in a network, communication and coordination occurs on the lower level. This is why a network appears flat in design. Since there is no "chain of command" for information to travel up and down, direct information flow can occur across and throughout the network. This creates more efficient information flow and interoperability among the nodes. In addition, counter-leadership targeting has little impact on the network since nodes are decentralized. With the advantages that the network holds over the hierarchy, it is clear that the best way to fight a network is with another network. This being said, it is also clear that mastering the network form of organization will give the ultimate advantage.[27]

E. SUMMARY

The Information Age is favoring network organizations more than ever before. The concept of Netwar has changed the world of conflict on a global level, and organizational adaptation must occur in order to keep up with the advances in information technology. In the missions of MHLS and MHLD, the enemy is moving towards the highly-efficient all-channel network design by using a hybrid of the hub and all-channel designs. The traditional hierarchy form will suffer continual defeats in the future if it encounters networked adversaries, given the information advances being made every day. The best way to effectively monitor and oppose networked terrorist organizations is to network the MHLS and MHLD intelligence mechanisms. The first to master the network organization will ultimately be successful in reaching its goals.

[27] Arquilla, 15.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. THE DOMESTIC MARITIME INTELLIGENCE NETWORK; ORGANIZING TO EFFECTIVELY MONITOR THE ENEMY

A. AN INTELLIGENCE NETWORK FOR MHLS AND MHLD

To keep up with the emerging domestic threat environment associated with Netwar, it is imperative that the intelligence support to MHLS and MHLD be organized with the ability to keep up with the enemy's terrorist network. By looking at the organizational structures of DHS and USNORTHCOM, it is clear that both organizations are hierarchal in form. It is also clear that the perceived enemy structure is highly networked. Based on discussions made earlier about the difficulty hierarchies have fighting networks, the best organizational method to counter the perceived enemy is to network the forces involved in defending against the threat.

While the operational structure should be adapted as well, the point of this research is to provide insights into networking the intelligence support to MHLS and MHLD. In order to effectively monitor and predict enemy actions that threaten the domestic maritime environment, a hybrid form of the all-channel network should be implemented in the domestic maritime intelligence organization supporting both missions. This network must have the capability to support the strategic, operational, and tactical levels within the domestic maritime environment. While support to each warfare level is not always clear and direct in an all-channel network, some dedicated support to each warfare level is important in order to provide continual situational awareness. This all-channel hybrid requires hub network components, and components capable of tailoring and filtering relevant intelligence for missions they support within the overall network.

B. THE FOUNDATION OF DOMESTIC MARITIME INTELLIGENCE

A joint-interagency environment is vital to building a domestic maritime intelligence network. The structure of joint-interagency relationships must formally exist in theory, doctrine, and practice. Culturally, this is a very difficult undertaking because the various hierarchal agencies within the U.S. government have traditions of competition with peer intelligence organizations. However, the reluctance to share intelligence, or

even identify a customer for certain intelligence, was a principal contributor to the outcome of the terrorist attacks of September 11, 2001.

The Joint Inter-Agency Task Force (JIATF) concept, which was implemented to support counter-drug operations, offers an approach that would work well for MHLS and MHLD intelligence as well. This design creates formal relationships between all agencies involved in the mission, and cements communication and liaison circuits into a network. Overall, three main ideas must be formally implemented in order to develop a foundation with which to build a domestic maritime intelligence network:

- Willingness to actively share information at all levels.
- Creation of formal liaison and interagency communication.
- Elimination of the competitive paradigm between intelligence agencies.

The sharing of information between various agencies is extremely important in the domestic maritime environment, given the many jurisdictions and agencies involved. Guidelines implemented by Intelligence Oversight and Posse Comatatus do not impact sharing information related to terrorist activity between law enforcement and intelligence organizations. Therefore, information sharing between these organizations can and must occur, in order to effectively monitor and predict terrorist actions. Failing to pass along relevant intelligence in a timely manner will create additional vulnerabilities as the terrorist networks adapt their swarming tactics to find perceived gaps in the intelligence flow.

The creation of formal liaison and communication between agencies is a necessary process in order to encourage and strengthen information sharing. Liaison allows for a direct communication path between agencies. It provides better knowledge of intelligence capabilities, and clearly defines relevant information from agency to agency. Communication and information systems must be standardized or made compatible from agency to agency as well. This will allow information to pass to the agency needing it, and is also a vital component of an all-channel network. Strong and frequent communication among all agencies will allow intelligence to flow with the speed and efficiency of the all-channel network.

Finally, competitive intelligence does not have any role in MHLS and MHLD. The past competition among intelligence agencies, for purposes such as recognition and

self-preservation, will only impede the efficiency of the intelligence network. The overall goal of MHLS and MHLD is to protect the homeland of the U.S. Therefore, regardless of the actual organization conducting the mission, intelligence support remains the same. An overall Maritime Domain Awareness (MDA) will be created. According to the Coast Guard, MDA is "the processing total awareness of vulnerabilities, threats, and targets of interest on the water".[28] Eliminating competition will ensure that both missions are supported with the same resources and professionalism.

C. STRATEGIC LEVEL INTELLIGENCE FUSION

Although the all-channel network allows direct communication between all nodes in the network, certain nodes must have dedicated missions to support the operations at each level of warfare. The primary node responsible for the fusion of intelligence at the strategic level should be the National Maritime Intelligence Center (NMIC). NMIC would be responsible for providing the strategic Common Intelligence Picture (CIP) of the domestic maritime situation to DHS, USNORTHCOM, and other strategically focused components of the network.

NMIC, located in Suitland, MD, conducts surveillance of the global maritime environment and provides analysis on trends within that environment. In addition, NMIC is a joint organization between Naval Intelligence and Coast Guard Intelligence. This creates a strong tie between strategic support to MHLS and MHLD because of the co-location of lead maritime intelligence elements of DHS and DOD. NMIC has a majority of naval intelligence assets and personnel associated with it. Due to its role of focusing on the global theater, as well as the domestic theater, it is best that NMIC continue to have a strong Naval Intelligence representation. With a global view of the maritime environment, NMIC is a natural choice to provide strategic maritime intelligence fusion to both DHS and USNORTHCOM.

NMIC currently maintains coordination with other intelligence agencies and some liaison officers as well. However, direct liaison with all strategic intelligence organizations should occur at NMIC. Representatives from agencies such as CIA, NSA, FBI should have a strong presence at NMIC, creating a strategic JIATF-type concept.

[28] USCG. "Homeland Security". www.uscg.mil. 2003.

This would encourage information sharing, and would bring about a better understanding of intelligence collection assets which the other agencies possess. In addition to liaison with the other agencies, common information technology should be implemented in order to efficiently pass the strategic CIP to all other agencies in the network. By pooling together various strategic intelligence resources for analysis and fusion, NMIC would give direct support to both DHS and USNORTHCOM through USCG HQ and NAVNORTH. In addition, as a node within the all-channel network, all elements in the network would be given an increase in level of intelligence support.

D. OPERATIONAL LEVEL INTELLIGENCE FUSION

The fusion of maritime intelligence at the operational level should primarily occur at the Maritime Intelligence Fusion Center (MIFC). Ideally, there should be two MIFC nodes, one to support each domestic maritime theater. Each should be responsible for developing the operational CIP within their respective theaters, and providing direct support to LANTAREA, PACAREA, NAVNORTHFLT-E, and NAVNORTHFLT-W.

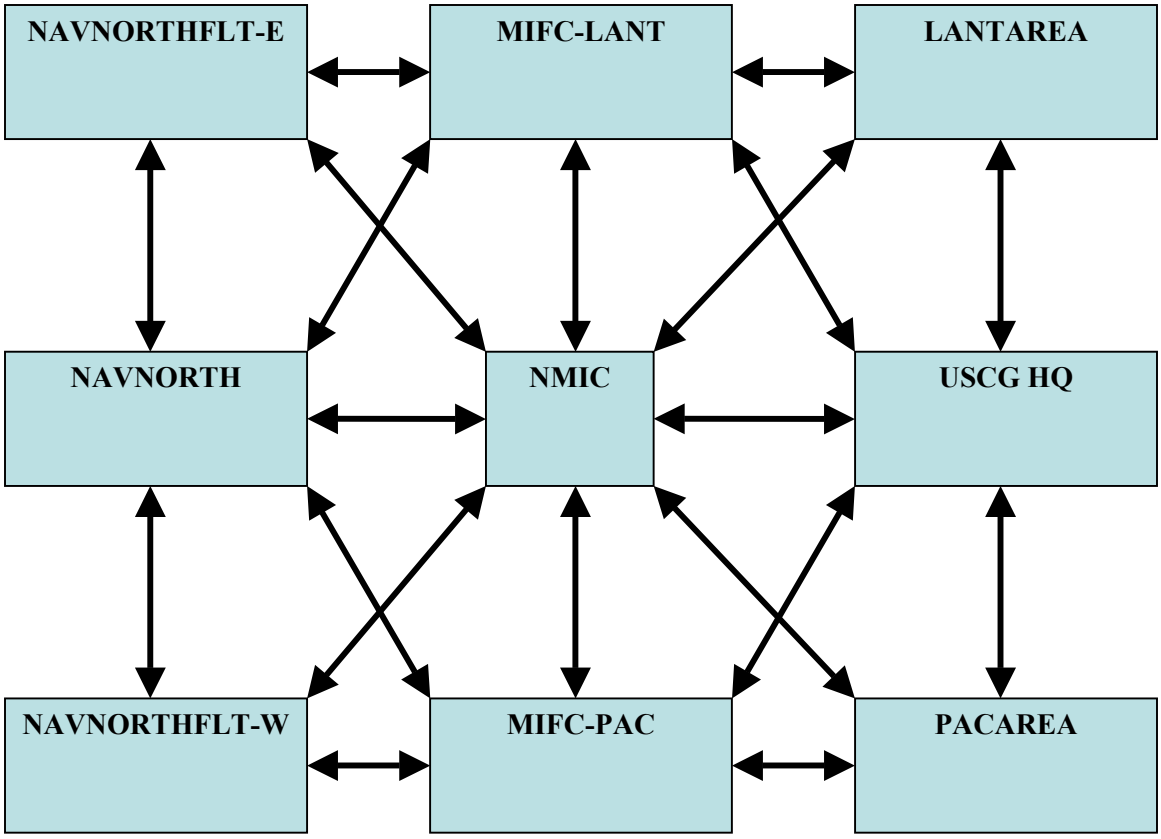
MIFC-PAC, currently operating in Alameda, CA, was established to support PACAREA operations. The east coast version, MIFC-LANT, is to be established in the fall of 2003 in Dam Neck, VA. These organizations are primarily manned and supported by USCG Intelligence assets. This is the best approach since these nodes concentrate mainly on the domestic maritime environment. Since the majority of intelligence personnel would be drawn from USCG, the MIFC would have no limitations on accepting information from both law enforcement and the foreign intelligence circuits, regardless of it being clearly associated with terrorism. However, these centers should be joint as well. Naval Intelligence should have a significant presence at each MIFC in order to facilitate transitions between MHLS and MHLD, and to ensure that the implementation of each mission can be supported effectively.

In addition, each MIFC should also represent a JIATF-like concept. Liaison officers from national intelligence agencies, as well as state and federal law enforcement, should be present in order to establish effective intelligence flow and information sharing. Any agency that can provide information on the operational maritime theater should have formal connections to each MIFC. Compatible interagency information

systems are important at this level as well. Each MIFC should coordinate directly with the other MIFC, NMIC, LANTAREA, PACAREA, and NAVNORTHFLT-E/W in order to develop the operational CIP. In addition, each MIFC would provide information to the all-channel network where overlaps between the warfare levels occur.

An example of how the strategic and operational networks fit together is presented in Figure 9. This is an all-channel design, and is difficult to present on a two-dimensional drawing due to its three-dimensional structure. While the figure does not necessarily illustrate the direct connection between all nodes, the three-dimensional interpretation of the figure connects each node to every other node in the network.

Figure 9. Strategic and Operational Level Domestic Maritime Intelligence Network Structure.



E. TACTICAL PORT LEVEL INTELLIGENCE FUSION

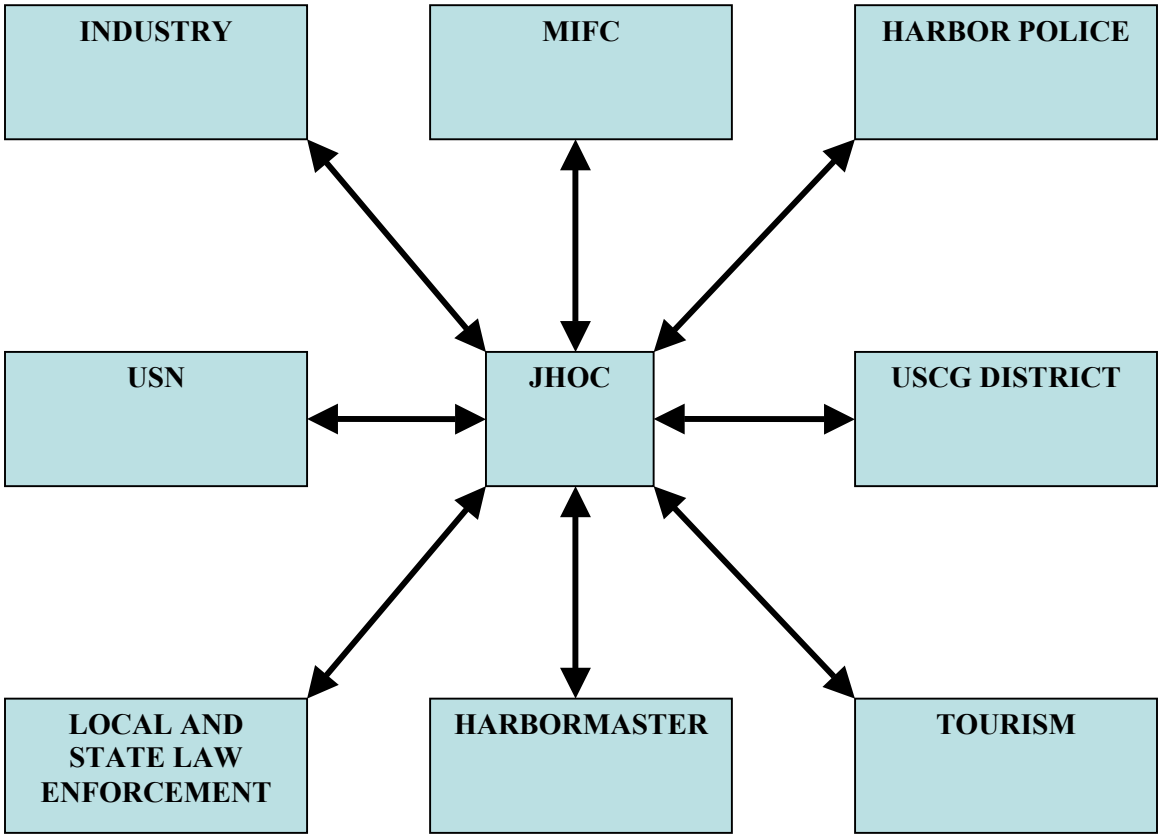
Tactical intelligence fusion with respect to MHLS and MHLD should mostly be done at the port level. USCG and USN assets conducting missions at sea will be supported by MIFC fusion, and the networking of organic intelligence elements within units themselves. At sea there are fewer overlaps in jurisdiction at the tactical level. Port security and defense, however, requires direct tactical fusion because of its unique environment. This thesis proposes that the best method for conducting this is to develop a Joint Harbor Operations Center (JHOC). The JHOC supports all elements within the port, and is operated under the Captain of the Port.

Currently, San Diego has a prototype JHOC operating under the Captain of the Port of San Diego. This JHOC was established to facilitate coordination between various

elements of the port. Practically speaking, each port should develop and operate a JHOC which is tailored to that specific port. It should be comprised of elements of Coast Guard Intelligence, harbor police, local and state law enforcement, private industry security services, and any other organizations associated with harbor operations in that port. Naval Intelligence assets and personnel should also be a part of the JHOC if the port has naval facilities. If no naval facilities are present, Naval Intelligence should at least have some liaison in case Naval Intelligence assets are needed in that port. An example of how a JHOC for a given port should look is presented in Figure 10.

The JHOC should provide direct indications and warning to various harbor security forces. Also, as a node within the all-channel network, the JHOC should connect directly with other JHOC units throughout the coastline. This node represents the hub network hybrid portion of the all-channel network. The JHOC is a hub where elements of a specific port's security interact and pass information. Communication and information sharing between operational and tactical levels is still important, as well as sharing between tactical port levels.

Figure 10. Tactical Port Level Domestic Maritime Intelligence Network Structure.



F. GAPS AND RECOMMENDATIONS IN CURRENT ORGANIZATION

In the two years since the terrorist attacks of September 11, 2003, there have been many changes implemented which have increased the country's ability to perform the missions of MHLS and MHLD. That being said, there are still many gaps in the current intelligence organization that supports these missions. There are three principal areas where the current organization falls short of being effective:

- Organizational structure
- Information systems
- Misconceptions of the missions

The structure of current domestic maritime intelligence is a hierarchy, not a network, so that represents the largest gap in the organization. There are, however, certain areas within the intelligence organization which are already forming hybrid hierarchy-network relationships. Examples of these areas are the new concepts of MIFC and JHOC. On all levels, many informal ties are being made between agency, law enforcement, and military personnel. These connections rely on personal relationships, and begin to weave the web of a network. While these personal relationships can provide short-term solutions, the connections should be made formal and be reflected in doctrine and practice. In order for this to be truly effective, there must be organizational change in order to facilitate this new environment.

It is surprising that the world of information systems impedes the progress of the intelligence organization performing MDA since the United States is creating most of the information technology with which the world operates. One would expect that the home country of this technology would benefit most from its progress. According to John Arquilla, there are three primary components of an information system; sensors, communications, and information input to weaponry.[29] Only the first two components will be discussed here since information input to weaponry is very operations intensive, and the focus of this research is on intelligence only.

While there are several gaps in domestic maritime sensors, one area stands out above all others in this research. Sensors are practically non-existent in shallow water acoustics. The potential underwater threat in domestic ports and coastal waters is significant and growing. New technology has resulted in mini-subs and swimmer delivery vehicles (SDV) becoming available on the open market at affordable prices. In addition, unmanned underwater vehicles (UUV) have become much more advanced and inexpensive in recent years. Currently, the U.S. has no effective capability to sense or prosecute these threats should they be employed in a threatening manner in domestic ports or coastal waters. In addition, underwater mine detection assets are very few, and often unavailable in many ports. With the abundance of economic, military, and even nuclear targets located in U.S. ports, shallow water acoustics represents a significant gap

[29] John Arquilla Class Discussion, Naval Postgraduate School. 2002-2003.

in sensing current threats. The only way to monitor and predict possible threats in this environment is to invest in sensors that cover the shallow water realm.

With regard to communications, there are still many problems in finding compatible means of passing information. While this situation is starting to improve, there are many legacy systems which provide little value added in the overall collection and dissemination of intelligence. These systems are incompatible with others, and definitely do not cross the lines of all agencies involved. Security clearances can be problematic at lower levels, and when interaction between intelligence agencies and law enforcement occur. This obstacle must be eliminated in order for the right group to see the information it needs to perform its mission in a timely manner. In addition, security on current communication systems is often neglected. Strong cryptology and information assurance is paramount in the increasingly complex world of information operations. In order to truly build an all-channel network, interoperability and security of communications must be established between every node or the whole network becomes ineffective and vulnerable. Creating interoperable communication systems, and protecting them with strong security mechanisms, is the only way to make the maritime intelligence network efficient.

There are a few misconceptions of the missions of MHLS and MHLD that exist as well. These misconceptions serve to detract from the overall mission effectiveness, and do not help the protection of the homeland of the United States. The first misconception is commonly made by older generations in the Navy. Many often treat MHLS and MHLD as the traditional mission of Anti-Terrorism Force Protection (ATFP). The title of this mission sounds adequate, however, the execution of this mission in the past emphasized the protection of military forces from terrorism. While preserving military forces is important, traditional ATFP cannot execute the missions of MHLS and MHLD. These two missions revolve around the idea of protecting the homeland and its citizens. Locking down bases and forces in order to protect them when a threat appears only makes the homeland itself more vulnerable to the swarming tactics of Netwar. The citizens of the United States expect that the military will protect them at home as well as away. In order for MHLS and MHLD to be executed to the greatest extent possible, the ATFP misconception must be eliminated at all levels.

The other misconception within MHLS and MHLD is the characterization of the threat. Within many maritime components of DHS and USNORTHCOM, the "asymmetric threat" is characterized as merchant shipping. While merchant shipping can represent a significant challenge to these missions, other areas such as underwater threats, mines, and maritime use of WMD need to be addressed as well. Simply focusing on one area within the missions once again allows the success of swarming tactics by terrorist groups.

G. SUMMARY

The emerging domestic threat environment associated with Netwar provides some serious challenges in the prosecution of the missions of MHLS and MHLD. To effectively support these missions, an all-channel hybrid network should be implemented for domestic maritime intelligence, with an emphasis on interagency architecture. Within this network, the principles of information sharing, liaison and communication, and elimination of competition between intelligence agencies must build a foundation upon which to operate. The networking of nodes such as NMIC, MIFC, and JHOC will allow proper support to be provided to each level of warfare, while ensuring that the overall network an still rapidly and efficiently operate. Only by implementing changes in organizational structure and information systems, and by clearing up misconceptions of the missions of MHLS and MHLD, can the overall network be created in a manner to effectively protect America's homeland.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION AND OVERALL SUMMARY

A. REVIEW

Throughout recent history, the United States has focused its Homeland Security and Defense missions away from the domestic theater. A new threat dimension has arisen from the Information Age, which now challenges the United States in its own backyard. The terrorist attacks of September 11, 2001 illustrate the seriousness of this new threat environment. Within this new atmosphere of significant domestic terrorist threat, the missions of MHLS and MHLD have risen in importance as never before. Intelligence support to each mission forces a significant change in the way that the intelligence community conducts business. A new way of organizing the intelligence community can yield significant advances in support to MHLS and MHLD. This reorganization must develop a highly networked domestic maritime intelligence community.

While the missions of HLS and HLD reflect certain differences in definition, the overall goal of each is to protect the homeland of the United States against terrorist attacks. The recent creations of DHS and USNORTHCOM have provided a C2 structure with which to conduct these two missions. Under each respective command, USCG has the lead for MHLS and NAVNORTH takes over when conducting MHLD. The resulting C2 organizations for both MHLS and MHLD are hierarchal in nature.

The theory of Netwar, as described by John Arquilla and David Ronfeldt, describes the evolution of network organizations based on advances made in the information revolution. This theory proposes a progression towards the complex all-channel network form. Hierarchies have significant difficulty fighting networks. Therefore, with the enemy defined as a hybrid all-channel terrorist network targeting the homeland of the U.S., it will become increasingly difficult for a hierarchal intelligence community to effectively monitor and predict this enemy's likely courses of action.

With all of these ideas put together, it is clear that organizational change must occur in intelligence support to MHLS and MHLD. This thesis argues that the most effective way to organize these intelligence communities is to merge them both into a domestic maritime intelligence network.

B. KEY POINTS

To monitor and predict enemy actions in MHLS and MHLD, a hybrid form of the all-channel network should be developed for use by the domestic maritime intelligence community. This network should be all-channel in form, with certain hub network nodes. In addition, the ability to tailor, filter, and fuse information at the strategic, operational, and tactical levels must be implemented. In order to effectively accomplish this task, domestic maritime intelligence must attain a joint-interagency form. The foundation beneath this intelligence network encompasses the formal implementation of three main ideas:

- Willingness to actively share information at all levels.
- Creation of formal liaison and interagency communication.
- Elimination of the competitive paradigm between intelligence agencies.

The implementation of these ideas will allow a hybrid all-channel network to form in support of MHLS and MHLD.

Within the network, each warfare level must be supported with dedicated intelligence fusion. NMIC should be a dedicated node within the network, responsible for fusing intelligence at the strategic level. MIFC-LANT and MIFC-PAC should be the two nodes in the network primarily focusing on fusion at the operational level. Finally, at the tactical port level, each port should have a JHOC which is responsible for monitoring activity within each port. As with the concept of the all-channel network, all of these nodes must become interconnected, so exchange of information can occur between all levels of intelligence support.

The current intelligence organization has three major issues which impact its ability to adequately support MHLS and MHLD:

- Organizational structure
- Information systems
- Misconceptions of the missions

Within each of these areas there are significant shortfalls which endanger the homeland maritime domain each day. By developing a maritime intelligence network, creating effective sensors and communications, and truly understanding the missions of MHLS

and MHLD, the country can begin to efficiently develop a safer domestic maritime domain.

C. THE FUTURE

As the Information Age continues to provide new information technologies, organizational practice in all aspects of life will move steadily towards the network principles. Each day new technologies emerge from the corporate sector and provide advanced information systems which are widely available, easily portable, and increasingly affordable. Within the past 15 years, information technologies such as laptop computers, internet, cellular telephones, and fax machines have been assimilated into practically every facet of life. As information technology develops, so will the network form of organization. Remaining hierarchies will suffer great disadvantages and defeats when encountering adversarial network organizations.

The willingness to adapt organizational structure in intelligence will pay great rewards in the future support to security and defense operations. Incorporating ever-evolving information technology into highly networked organizations will pave the way for progress in the future. "He who will not risk, cannot win" was uttered long ago by John Paul Jones. However, his words still ring true today in a world which is becoming increasingly complex and forever changed by the Information Age.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Professor Dan C. Boger
   Department of Information Sciences
   Naval Postgraduate School
   Monterey, California

4. Professor R. Mitchell Brown
   Naval War College
   Monterey Campus, Naval Postgraduate School
   Monterey, California

5. Bradley J. Storey
   COMPACFLT N2
   Pearl Harbor, Hawaii

6. Professor John Arquilla
   Naval Postgraduate School
   Department of Defense Analysis
   Monterey, California

7. Professor James Wilson
   Naval Postgraduate School
   Department of Oceanography
   Monterey, California

8. Professor Robert Bourke
   Naval Postgraduate School
   Department of Oceanography
   Monterey, California